IVV 09-9: Safety and Mission Assurance

Version: E

Effective Date: January 31, 2018

Note: The official version of this document is maintained in IV&V's internal IV&V Management System Website (https://confluence.ivv.nasa.gov:8445/display/IMS). This document is uncontrolled when printed.

Purpose

The purpose of this system level procedure (SLP) is to document and establish a consistent method for performing tasks assigned to the IV&V Safety and Mission Assurance (SMA) Support Office (SSO).

Scope

This SLP addresses SSO team member planning, scoping, performing, reviewing and delivering of the SMA products/services.

Definitions and Acronyms

Official NASA IV&V roles and terms are defined in the Quality Manual. Specialized definitions identified in this SLP are defined below.

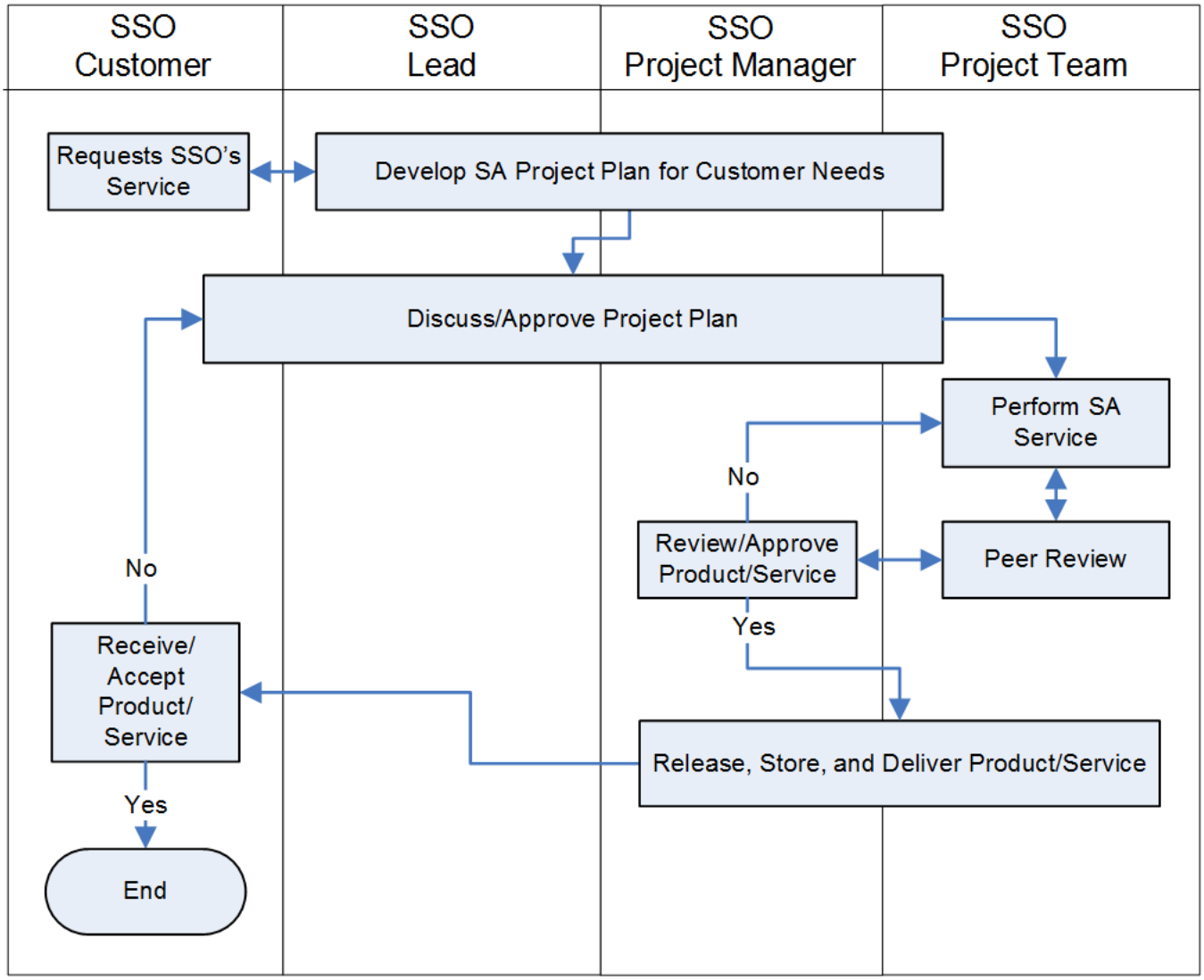
- **Scope of Work**
  - Scope of Work is an agreement that represents the size/extent of work to be performed by the SSO for its customers and is documented in the Project Plan.
- **Project Plan**
  - The Project Plan is a document/record that captures and summarizes the safety and mission assurance efforts associated with each SSO project/task. This document covers the scope of work, objectives, planned activities, rules of engagement, needs, and contact list. It is updated as needed to reflect changes in scope.

Acronyms

CAR	Corrective Action Request
CNSI	Classified National Security Information
DRD	Data Requirements Document
ECM	Enterprise Content Management
FTA	Fault Tree Analysis
IMS	NASA IV&V Management System
NODIS	NASA Online Directives Information System
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
OCE	Office of the Chief Engineer
OSMA	Office of Safety and Mission Assurance
PHA	Preliminary Hazard Analysis
SA	Software Assurance
SLP	System Level Procedure
SMA	Safety and Mission Assurance
SSO	SMA Support Office
STD	Standard
STEP	SMA Technical Excellence Program
SWHA	Software Hazard Analysis

Process Flow Diagram

The following diagram depicts process of planning, scoping, performing, reviewing, and delivering of the SMA products/services described in this document, and the responsibilities and actions that shall be performed by process participants. Any information supplemental to the depicted process will appear after the diagram.



IVV 09-9 Process Flow Diagram 2018-01-31.vsd

The IV&V SMA Support Office Lead pre-plans, coordinates, and identifies potential customers in need of software assurance services/products and contacts the appropriate customer's representatives to discuss and identify specific software assurance needs and available services/products. Once it is determined services/products are needed, a plan is developed and the scope of work is negotiated and agreed upon with the customer(s), then documented in the Project Plan. The development of the Project Plan is an iterative process, and the Project Plan is updated annually in support of the IV&V Program budgeting and resource allocation process. Additionally, the Project Plan is updated as needed to document and coordinate programmatically any scope changes. The SSO team assigned to the task executes the activities necessary to perform the required services and develop the products. Execution and status of the task is recorded in Enterprise Content Management (ECM). When the services/products are completed, a peer review is conducted utilizing an iterative process to disposition comments/changes prior to SSO Project Manager review and approval. Once approved the product(s) are saved in ECM and delivered to the customer for acceptance. SSO will manage risks in accordance with IVV 22, *Risk Management*.

Products containing CNSI shall be handled according to S3007, *IV&V Guidelines for Handling CNSI*.

SMA Product /Services

Software Hazard Analysis (SWHA)

The SMA Support Office performs analysis on safety and mission critical software to identify and trace software that controls, mitigates, and contributes to the hazards outlined in the Preliminary Hazard Analysis (PHA). SSO performs SWHA from a systems view and, when appropriate, performs SWHA in parallel or in conjunction with personnel performing the hardware hazard analysis. This parallel effort could include generating a single fault tree analysis (FTA) covering both hardware and software faults as well as producing joint hazard reports. A summary of the SWHA products include: FTA reports with fault trees, hazard reports, trace matrices, verification checklists, etc. as defined in the project software safety and/or assurance plan.

Software Assurance (SA) Plan Development

The SMA Support Office supports the development of project Software Assurance and Safety Plans. These plans delineate the SA activities for the software development and maintenance activities required throughout the lifecycle of a project, ultimately to assure software's contribution to safety and quality. The primary focus of this effort is to provide a plan or product that is approximately 95% complete to be formalized and approved by the customer/project team.

Software Standards Update & Review

The SSO works closely with NASA Headquarters to aid in the development, update and review of agency software standards. The primary focus of the effort is to review and facilitate the development and/or update of new and existing agency software standards. The SSO also provides assessments of current industry standards sharing NASA's perspective with industry's standard developers and supports the development of these standards and alternatively incorporates industry's perspectives as applicable.

NASA Procedural Requirements Handbook Development

The SSO works closely with NASA Headquarters to aid in the development and updating of agency NASA Procedural Handbooks. The primary focus of the effort is to develop/update new and existing agency handbooks. The activities include supporting the collection and formulation of data to be used to update handbooks and in some instances create a web based electronic handbook.

Data Requirements Document (DRD) Analysis

The SSO performs analysis of DRDs to ensure that all the necessary information and artifacts needed by the NASA IV&V Program will be made programmatically and/or contractually available by missions/projects selected to receive IV&V services. A secondary objective is to ensure that projects create and deliver artifacts required for SMA. The analysis results will be summarized and reported to the mission/project (DRD owner) and the appropriate center SMA organization.

Software Assurance Product Assurance

The SSO reviews the required project documentation relative to project requirements and NASA-STD-8739.8, *NASA Software Assurance Standard*. This effort assures that the SA plan, products and related documentation adhere to the project software management plan and comply with the agency standard, project requirements, and associated contract(s).

Information Assurance (IA) Security Analysis

The SSO performs full-lifecycle (i.e., Concept to Deployment) Information Assurance (IA) security analysis to ensure the logical and systematic conversion of customer or product requirements into total secure systems solutions that acknowledge technical constraints. Independent assessments (e.g., system and software security vulnerability, threat, and risk assessments) and penetration tests are conducted on development and large-scale operational environments.

Control of Nonconforming Product

If the SSO identifies a problem with a Product that has already been delivered to the customer, the SSO Office lead shall immediately inform the Point of Contact (POC) of the problem. If the customer identifies a product produced by the SSO as nonconforming (e.g., in an inappropriate format or performed on the wrong project artifact), the SSO Office Lead shall resolve the issue with the customer.

The SSO Office lead shall determine if the problem is noteworthy of a Corrective Action Request (CAR) per IVV 14, *Corrective and Preventative Action*. Regardless of how the problem has been identified, the SSO Office Lead shall:

- Ensure that the problem is resolved and that the customer is provided a full explanation of events
- If a CAR was generated, request closure of the CAR once the nonconforming product has been approved and sent to the customer

The nonconforming product shall be subjected to its established verification process once the nonconforming product has been corrected.

Metrics

Any metrics associated with this SLP are established and tracked within the NASA IV&V Metrics Program. Metrics and data to support SMA Support Office goals will be captured and reported per IVV 12, *NASA IV&V Metrics.*

Records

The following records will be generated or updated and filed in accordance with this SLP and IVV 16, *Control of Records*, and in reference to NASA Procedural Requirements (NPR) 1441.1, *NASA Records Management Program Requirements*.

Record Name	Original	Vital	Responsible Person	Retention Requirement	Location
Project Plan	Y	N	SMA Support Office Lead	Destroy/delete between 0 and 30 years after cutoff. (8/103)	ECM*

SSO Products	Y	N	SMA Support Office Lead	Destroy/delete between 0 and 30 years after cutoff. (8/103)	ECM*

*Products containing CNSI shall be handled according to S3007, *IV&V Guidelines for Handling CNSI*.

References

REFERENCES	
Document ID/Link	**Title**
IVV QM	NASA IV&V Quality Manual
IVV 12	NASA IV&V Metrics
IVV 14	Corrective and Preventative Action
IVV 16	Control of Records
IVV 22	Risk Management
NPD 7120.4	NASA Engineering and Program/Project Management Policy
NPD 8700.1	NASA Policy for Safety and Mission Success
NPR 1441.1	NASA Records Management Program Requirements
NPR 7150.2	NASA Software Engineering Requirements
NASA-STD-8719.13	NASA Software Safety Standard
NASA-STD-8739.8	NASA Software Assurance Standard
S3007	IV&V Guidelines for Handling CNSI

If any procedure, method, or step in this document conflicts with any document in the NASA Online Directives Information System (NODIS), this document shall be superseded by the NODIS document. Any external reference shall be monitored by the Document Owner for current versioning.

Version History

VERSION HISTORY

Version	Description of Change	Rationale for Change	Author	Effective Date
Basic	Initial Release		Steve Husty	10/25/2010
A	Updates to match actual procedures		Scott Kinney	8/6/2012
B	Update and clarify	in response to internal audit suggestions	Scott Kinney	10/26/2012

C	ISO 17020 requires that an organization document the activities for which it is competent. IVV 09-9 already includes a list of products/ services in Section 4.1. To satisfy the ISO requirement, update this list to include IA /security assessments/ cloud services.	In support of the following ISO 17020 requirement: 1) Requirement 5.1.3 - The inspection body shall have documentation which describes the activities for which it is competent. ISO 17020 certification is required for the FedRAMP 3PAO certification that the IV&V Program is pursuing.	W. Greg Stine	4/6/2015
D	Add section on “Control of Nonconforming Product” with optional CAR creation.	PAR 2015-P-441: To meet ISO 9001 requirements and add consistency with IVV 09-4, Project Management.	Ken Rehm	1/27/2016
E	Project Plan replaces Task Summary. Use ECM to document records. Product Log is removed. Updated Process Flow replacing Project Owner with Project Manager and Project Team. Added CNSI requirement and reference to S3007.	Historically, the Task Summary has contained both plans and a status of activities performed. Now implementing a new approach where the scope, objectives, and planned activities are captured in one document and the work performed is captured elsewhere. Moving toward using JIRA for task management. Some work may contain CNSI.	Scott Kinney	1/31/2018